SECURING DISTRIBUTABLE CONTENT AGAINST HOSTILE ATTACKS

Abstract of the Disclosure

In one embodiment, the present invention may perform a transformation based on existing program operations or operators which may provide encrypting compiler-generated code for compilation with original source code, securing distributable content in hostile environments. As an example, use of compiler analysis and heuristics for pairing variables and identifying encryption/decryption points may protect distributable software, such as the compiled code from automated attacks. In one embodiment, pre-compiler software may dynamically obtain one or more program operators from the source code for applying data transformation based on custom ciphers to encrypt/decrypt data in between references to data variables in a particular portion of the source code, providing encrypting compiler-generated code for mixing with the source code prior to compilation into tamper-resistant object code.